#Configurazione# Configurazione di un Destination NAT (DNAT) su Sangfor NGAF V8.0.85

***Prodotto:** NGAF

***Versione:** 8.0.85

*1. Introduzione

1.1 Scenario

Sangfor DNAT (Destination Network Address Translation) è una funzionalità presente sui prodotti Sangfor IAM (Internet Access Management) e NGFW (Next-Generation Firewall).

DNAT (Destination Network Address Translation) è un metodo di routing utilizzato per permettere ad un firewall di tradurre un ip di destinazione in un altro ip di destinazione.

DI seguito vengono riportati dei punti chiave riguardo Sangfor DNAT:

- Viene usato per reindirizzare il traffico in arrivo su un host od un server specifico all'interno della rete locale.
- Viene spesso usato per dare accesso dall'esterno a dispositivi che sono nella rete locale.
- Può essere configurato nelle interfacce web dei prodotti Sangfor IAM ed NGFW.
- La configurazione permette di impostare l'ip originale con relativa porta di destinazione e l'ip e porta di destinazione finale di traduzione.
- Questo aspetto è utile per scenari in cui si vuole esporre un servizio od un'applicazione locale su internet.

Di seguito in questa guida, vedremo i passaggi da seguire per pubblicare una risorsa locale.

1.2 Requisiti

1. Firewall Sangfor NGAF aggiornato all'ultima versione

2. Indirizzo ip e porta usati dalla risorsa locale che si vuole dare accesso dall'esterno

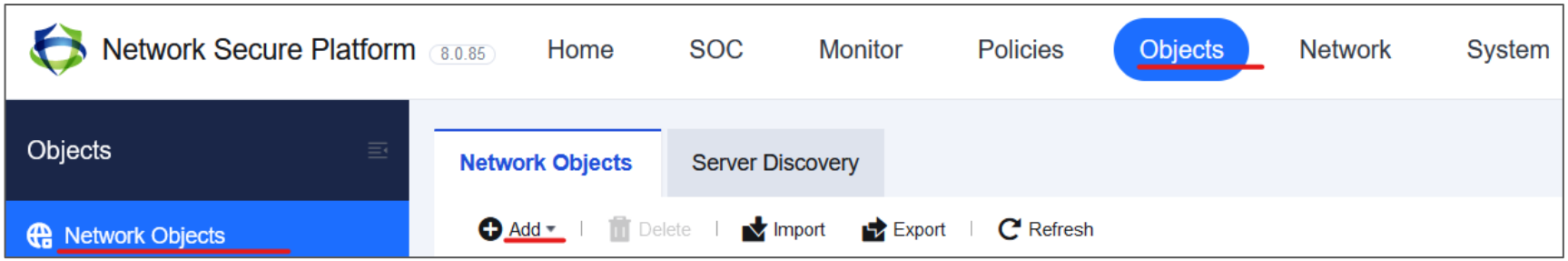
*2. Configurazione

In questa guida, abbiamo la rete locale 10.0.0.0/24 e si vuole pubblicare un server web locale (apache2) raggiungibile internamente con l'ip 10.0.0.5 sulla porta 20443

2.1 Configurazione DNAT NGAF DNAT

Passo 1. Controllare attentamente le zone definite nel firewall e configurare I relativi oggetti di rete su NGAF.

Per far ciò, occorre recarsi nella seguente sezione di NGAF:



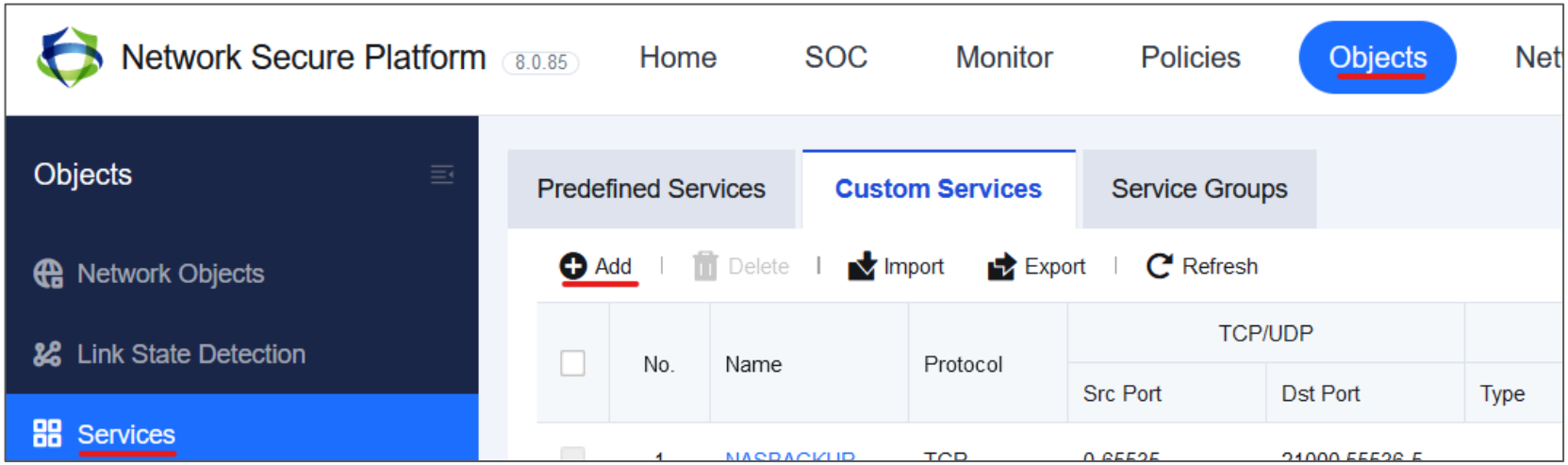
In questo esempio abbiamo:

Zona Sorgente: L3_WAN (la nostra wan)

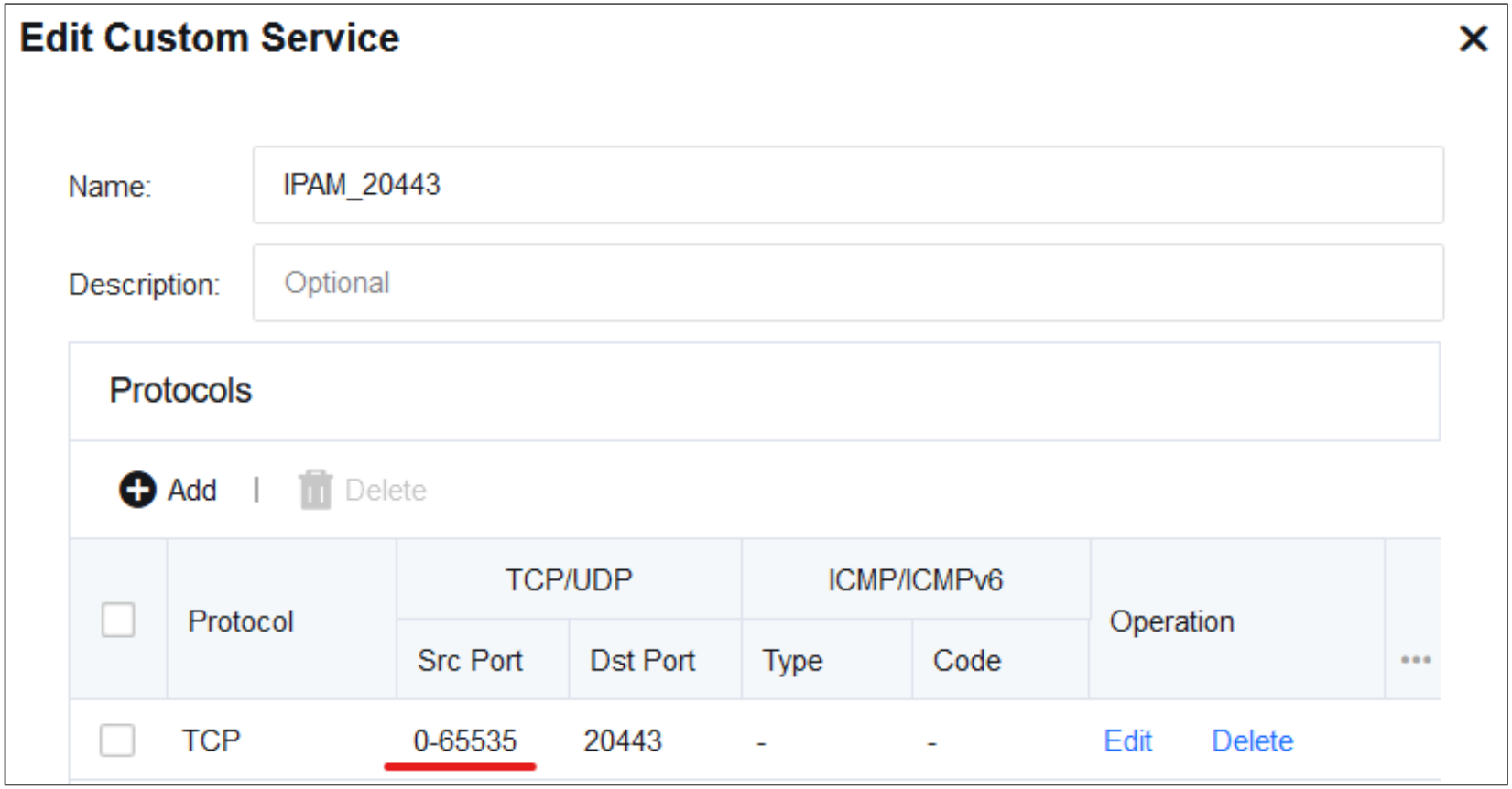
IP Pubblico: UTGNET (il nostro provider)

L'ip del webserver locale: PHPIPAM (il nostro webserver che si vuole pubblicare)

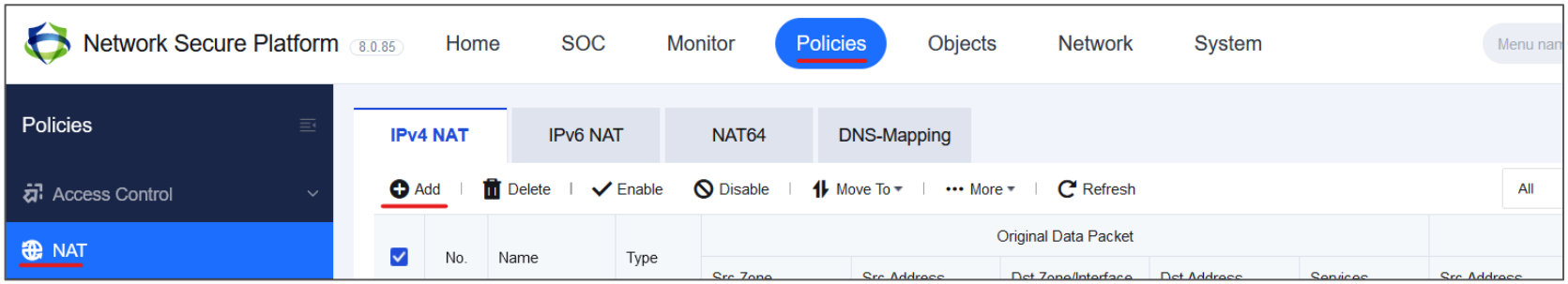
Passo 2. Creare un oggetto servizio custom dato che dobbiamo usare la porta 20443 TCP. Per far ciò, occorre recarsi nella seguente sezione di NGAF:



Nel nostro esempio ho creato un oggetto servizio custom chiamato IPAM_20443



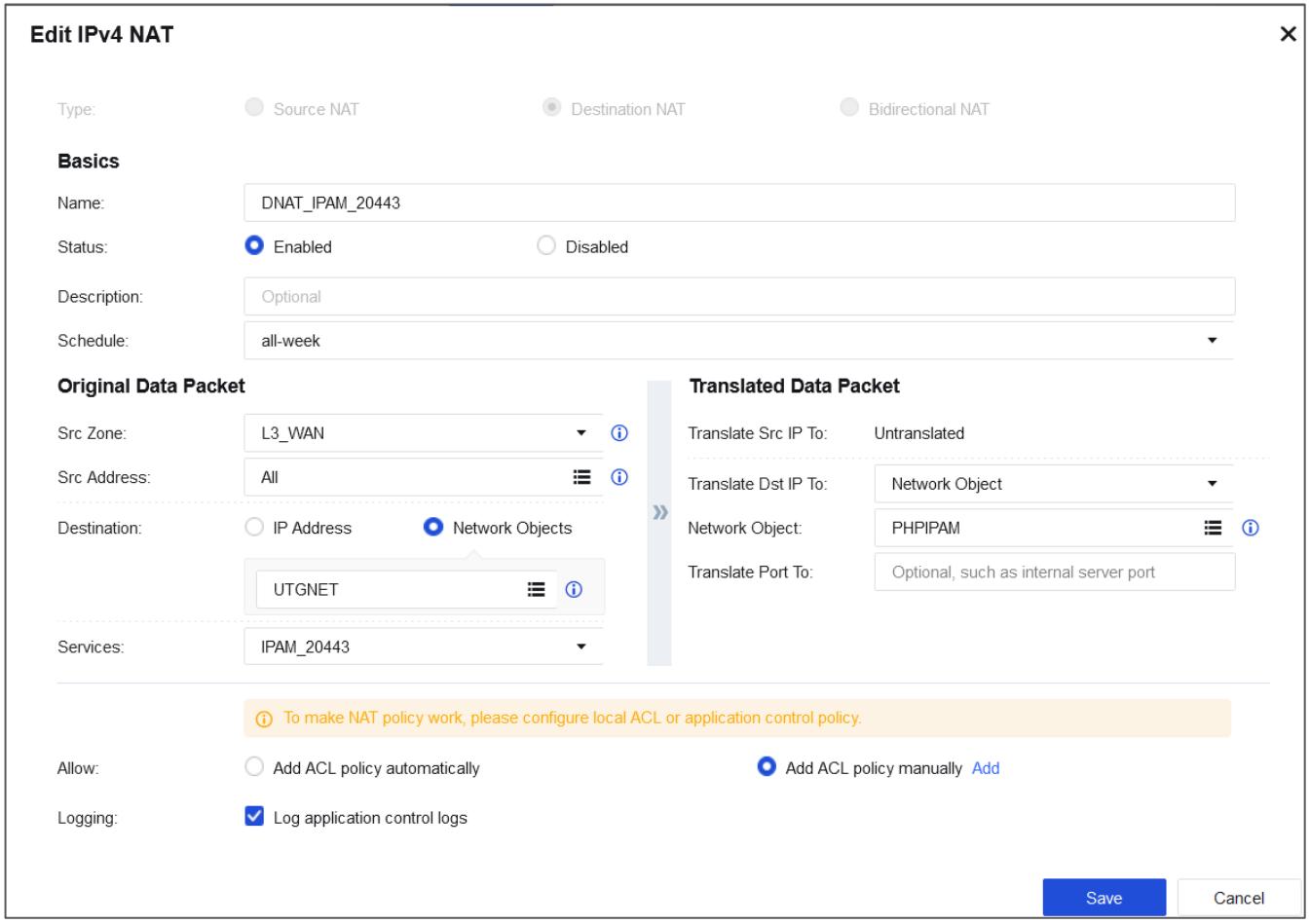
Passo 3. Creare ora un oggetto DNAT nella seguente sezione:



Selezionare Destination NAT uando gli oggetti creati nei passi precedenti.

Di seguito potete vedere che non uso una porta interna diversa dalla porta esterna.

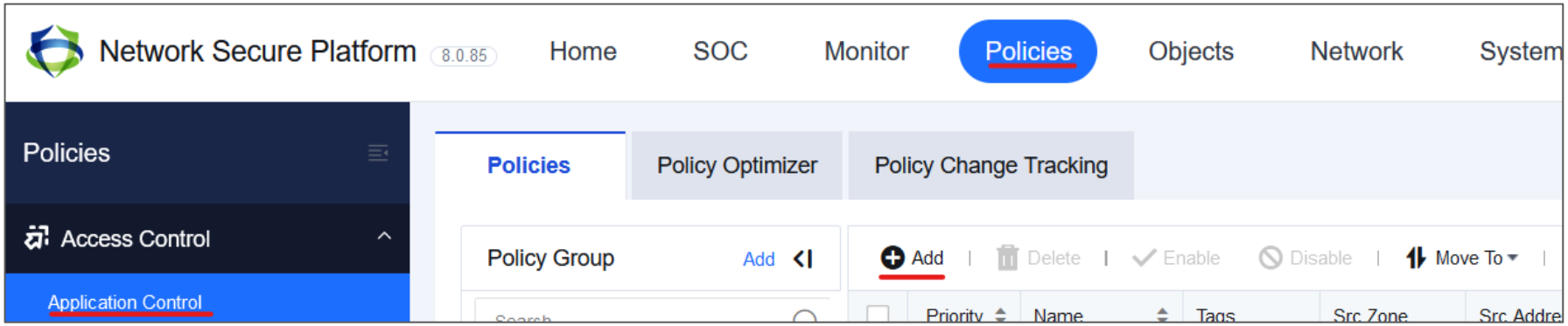
Di conseguenza, lascio bianco il campo Translate Port to



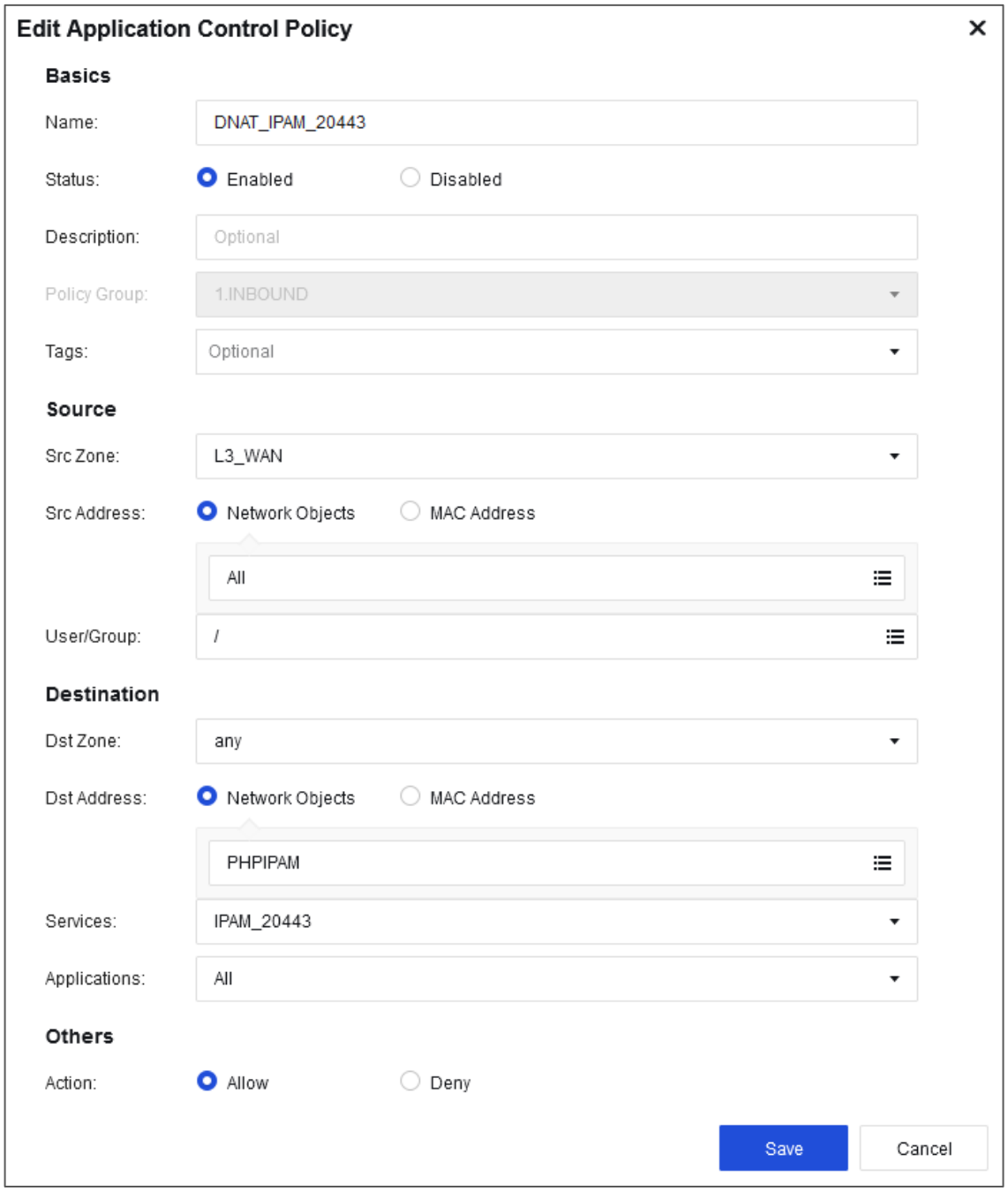
2.2 Configurazione policy NGAF

Passo 1. Nell'ultimo passaggio, se si sceglie di aggiungere automaticamente la policy ACL (Add ACL Policy automatically), si verrà reindirizzati nella sezione relativa alle policy dell'interfaccia web di NGAF.

Personalmente suggerisco di creare manualmente la policy su NGAF come segue:



Nel nostro esempio, ho creato una regola di controllo applicativa (application control rule) come segue:


Edit Application Control Policy
Basics
Name:
DNAT_IPAM_20443
Status:
Enabled
Disabled
Description:
Optional
Policy Group:
1.INBOUND
Tags:
Optional
Source
Src Zone:
L3_WAN
Src Address:
Network Objects
MAC Address
All
User/Group:
/
Destination
Dst Zone:
any
Dst Address:
Network Objects
MAC Address
PHPIPAM
Services:
IPAM_20443
Applications:
All
Others
Action:
Allow
Deny
Save
Cancel

*3. Attenzione

Quando si crea un oggetto service custom, è importante specificare 0-65535 come intervallo di porte sorgente, dato che non si può sapere la porta che viene usata dall’esterno per accedere alla risorsa pubblicata.